REMARKS

The Applicants thank the Examiner for performing a thorough search.

ISSUES RELATING TO PRIOR ART

A. Independent Claims 1, 10, 19, and 26. Claims 1-30 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Dondeti et al., U.S. Pat. No. 6,240,188 B1 (hereinafter Dondeti), in view of O'Toole, Jr. et al., U.S. Pat. No. 6,279,112 B1 (hereinafter O'Toole). The rejection is respectfully traversed.

To set forth a proper *prima facie* case of obviousness under § 103, the Office is required to present one or more references that show each and every element and limitation of the claims, and suggest the desirability and thus the obviousness of making the combination. The factual inquiry as to whether the references provide a teaching, motivation, or suggesion to combine references must be "thorough and searching," and specific reasons must be explained. In re Lee, 61 USPQ 2d 1430 (Fed. Cir. 2002). "The claimed invention must be considered as a whole ... the references must be viewed without the benefit of hindsight vision afforded by the claimed invention ..." Hodosh v. Block Drug Co., 786 F.2d 1136, 1143 n.5, 229 USPQ 182, 187 n.5 (Fed. Cir. 1986). The cited references are insufficient to establish obviousness.

The Office Action contends that Dondeti discloses "an event server," which determines whether publishers and subscribers are authorized to process certain events, and which generates an encrypted group session key for establishing one of the multicast groups. This is incorrect. Dondeti teaches a secure group communication system based on a distributed tree-based key management scheme. However, Dondeti has no teaching of an event server as claimed.

The concept of event services is well understood in the art. An information disclosure statement has been filed with this response. The references cited in the information disclosure

statement have been provided for the purpose of explaining event services as that concept would have been understood by a person of ordinary skill in the art when this application was filed. Specifically, event services are described on pages 319-324 of Understanding Microsoft Windows 2000 Distributed Services, on page 488 of Client/Server Survival Guide, and pages 448-449 of The Essential Distributed Objects Survival Guide. Many other cumulative references are believed to exist. A commercial vendor of event servers is The Information Bus Company (TIBCO).

Events are multicasted messages. An event server, as described in independent claims 1, 10, 19, and 26, establishes secure channels among multicast group members (such as routers in a packet-switched network) and manages group session keys for publishers and subscribers. Publishers and subscribers may register their interest in specific events with the event server, which checks whether a producer is allowed to produce a particular event and whether a subscriber is allowed to receive a particular event. The event server generates and distributes group session keys for establishing multicast groups that use encrypted communications. A publisher sends an event to the event server, which uses a group session key to authenticate and protect the multicast transmission to the event's subscribers. Event servers are not used in any prior approach to establish multicast group keys.

Dondeti does not disclose, teach or suggest an event server. The cited passage describes "a distributed tree-based key management scheme." Dondeti, col. 3, line 23-24. Applicants have carefully reviewed the cited portions of Dondeti and found nothing that teaches an event server. In fact, the cited passage describes a system that "delegates group control responsibilities and key distribution tasks evenly to the members," Dondeti, col. 3, line 26-28, which teaches

away from the claims because members, not an event server, are said to distribute keys. Dondeti fails to disclose an event server that handles these tasks on behalf of group members.

Moreover, Dondetti teaches against the methodology of group control that is implemented by an event server: "some form of centralized group control" is stated to be "a common failing" in secure communication systems between many senders and many members under the mistaken belief that all such systems are prone to a single point of failure and are not efficiently scalable. Dondeti, col. 1, line 25-28; Dondeti, col. 2, line 20-34.

Independent claims 1, 10, 19, and 26 recite, among other features, use of an event server that generates group session keys and distribute these keys to subscribers of an event or message (i.e. to group members). In contrast, each group member in Dondeti must independently compute a root key, which is used to encrypt and decrypt multicast data, by using the keys of all nodes in a path to the root as well as the keys of siblings of nodes in a path to the root. Dondeti, col. 4, line 11-19; Dondeti, col. 9, line 56-57. Further, an event server as claimed allows a publisher (sender) to target a message only to the event server, which will multicast the message to event subscribers. In contrast, in Dondeti a sender must multicast the message itself, Dondeti, col. 9, line 57-59, without taking advantage of secure multicast services provided by an event server.

For at least the reasons given above, Dondeti does not teach an event server. Therefore, Dondeti, even in combination with O'Toole, Jr., cannot and does not in any way disclose, teach, or suggest a feature recited by independent claims 1, 10, 19, and 26. Since a significant feature of Applicants' claims are missing in the combination of Dondeti and O'Toole, Jr., a rejection under 35 U.S.C. § 103(a) is not supported.

Accordingly, the rejection of Claims 1, 10, 19, and 26 is insufficient to set forth a *prima facie* case of obviousness, and should be withdrawn.

B. Dependent Claims

Claims 2-9, 11-18, 20-25, and 27-30 are dependent claims, each of which depends (directly or indirectly) on one of the claims discussed above. Each of Claims 2-9, 11-18, 20-25, and 27-30 is therefore allowable for the reasons given above for the claim on which it depends. In addition, each of Claims 2-9, 11-18, 20-25, and 27-30 introduces one or more additional features that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of all such features is not included at this time.

For all the foregoing reasons, Claims 1-30 are believed to be in allowable condition.

III. CONCLUSIONS & MISCELLANEOUS

The amendment herein is provided to more particularly and distinctly claim what is regarded as the invention. No new matter is introduced. Entry and consideration in due course are respectfully requested.

The Commissioner is hereby authorized to charge any shortage in fees due in connection with the filing of this paper, including extension of time fees, to Deposit Account 50-1302 and to credit any excess fees to such deposit account.

Respectfully submitted,

HICKMAN PALERMO TRUONG & BECKER LLP

Dated: August 14, 2002

Christopher J. Palermo
Registration No. 42,056

1600 Willow Street
San Jose, California 95125-5106
(408) 414-1202 CJP/AT/ta
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Box Non-Fee Amendment, Commissioner for Patents, Washington, D.C. 20231
on August 14, 2002 by
Teresa Austin

MARKED-UP COPY OF SPECIFICATION

1. Please replace the third paragraph on page 2, which starts on line 16, with the following new paragraph:

FIG. 9 is a block diagram of a computer system on which embodiments of the event service node may be implemented according to embodiments of the present invention.

2. Please replace the fifth paragraph on page 27, which starts on line 21, with the following new paragraph:

FIG. 5C shows the format of a reregister message. The reregister message shows each of the fields shown in FIG. 5B with the exception of the [Initialized] Wrap Token field. The reregister message comprises a Protocol Version field, a Message Type field, a Message Length field, an Initialize Token field, a Wrap Token Length field, and a four byte Interval Period field. The Interval [Field] Period value specifies a random duration for a group member to attempt to reregister. The default of the interval field is 0, indicating that the group member should immediately reregister.

3. Please replace the second paragraph on page 26, which starts on line 5, with the following new paragraph:

Under the above approach to key update, one of the subscribers 711, [719] 715 may receive an event message with an advanced key version indicating that it needs to reregister. Also, one subscriber 711, 715 may reregister with an event server 707a that has not received the key update. This is possible, for instance, when the process of replicating the directory servers has not finished. In this case, the subscriber 711 or 715 should reregister with the master event

server 707a for the particular event type. However, if the [reregistration] re-registration process fails, subscriber 711, 715 will proceed to a different event server 701a. The re-registration process could fail, for example, if the master event server 707a is down.

MARKED-UP COPY OF AMENDED CLAIMS

1. (Amended) A method for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, wherein each of the subscriber nodes and the publisher nodes receives a unique private key and that can determine events that the subscribers and the publishers may process, the method comprising the steps of:

registering the subscribers and the publishers with an event server configured to determine whether the publishers are authorized to produce certain events corresponding to [the] event types and whether the subscribers are authorized to receive the certain events in response to the step of [accessing] registering; and

generating, with the event server, a group session key for establishing [one of] the multicast [groups] group, the group session key being encrypted in a first message that has a prescribed format.

2. (Amended) The method as recited in Claim 1, further comprising the steps of:

receiving a second message from the subscribers in response to the subscribers determining whether the [received] first message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

3. (Amended) The method as recited in Claim 1, wherein the prescribed format of the first message conforms with lightweight directory access protocol (LDAP).

4. (Amended) The method as recited in Claim 1, wherein the prescribed format of the first message comprises a protocol version number field, a message type field, and a message length field.

5. (Amended) The method as recited in Claim 1, wherein the [step of authenticating comprises] directory authenticates by controlling access [by the directory] in conjunction with utilizing an external authentication service that allows extending membership of the multicast [groups] group to subscribers with no corresponding objects in the directory.

6. (Amended) The method as recited in Claim [1] 5, wherein the external authentication service is supplied by a Kerberos server.

7. (Unamended) The method as recited in Claim 1, wherein the event server manages the private keys of the subscribers and the publishers.

8. (Amended) The method as recited in Claim [1] 2, wherein the step of updating comprises:

creating a new group session key;

modifying [the objects] an object in the directory based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

9. (Unamended) The method as recited in Claim 1, wherein the step of registering comprises performing access control check of the subscribers by the event server.

10. (Amended) A communication system for creating a plurality of secure multicast groups in a network that includes a plurality of principals configured for functioning as [a subscriber] subscribers and [a publisher] publishers, each of the principals having a private key, a multi-master directory comprising a directory server for communicating with one or more of the principals to authenticate each of the principals and to provide access control, the multi-master directory controlling access on a per object and per attribute basis, the communication system comprising:

an event server coupled to the plurality of principals for registering the plurality of principals and for determining whether the principals are authorized to produce certain events when the principals are functioning as publishers and whether the principals are authorized to receive the certain events when the principals are functioning as subscribers; and

means in the event server for creating a group session key for establishing one of the multicast groups, by distributing the group session key in an encrypted

message to the subscribers, the encrypted message encapsulating the group session key according to a prescribed format;

means in the event server for updating the group session key by utilizing a change password protocol to modify an object in the directory;

means in the event server for notifying the subscribers to reregister in response to the updating of the group session key.

11. (Unamended) The communication system as recited in Claim 10, wherein the directory server is collocated with the event server, the directory server and the event server participating in a common one of the multicast groups.

12. (Unamended) The communication system as recited in Claim 10, wherein the prescribed format of the message conforms with lightweight directory access protocol (LDAP).

13. (Unamended) The communication system as recited in Claim 10, wherein the directory authenticates by controlling access in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

14. (Unamended) The communication system as recited in Claim 13, wherein the external authentication service is supplied by a Kerberos server.

15. (Unamended) The communication system as recited in Claim 10, wherein the prescribed format of the message comprises a protocol version number field, a message type field, and a message length field.

16. (Unamended) The communication system as recited in Claim 10, wherein the event server manages the private keys.

17. (Amended) The communication system as recited in Claim 10, wherein the event server updates the group session key by performing the steps of:
creating a new group session key;
modifying the [objects] object based upon the new group session key by using [a] the change password protocol;
sending a new message that contains the new group session key to the subscribers; and
notifying the subscribers to reregister.

18. (Unamended) The communication system as recited in Claim 10, wherein the event server performs access control check of the subscribers during registration of the subscribers.

19. (Amended) A computer system functioning as an event server and for establishing multiple secure multicast groups, the computer system comprising:
a communication interface for communicating with a plurality of nodes and for interfacing a multi-master directory to authenticate the computer system and

the plurality of nodes, the multi-master directory having access controls on a per object and per attribute basis, wherein the nodes access the directory to determine events that the nodes may process;

a bus coupled to the communication interface for transferring data;

an event server comprising one or more processors;

the one or more processors coupled to the bus for selectively generating a group session key and private keys corresponding to the plurality of nodes, the group session key being updated by utilizing a change password protocol to modify an object corresponding to the events in the directory;

an event server that is executed by the one or more processors; and

a memory coupled to the one or more processors via the bus, the memory including one or more sequences of instructions which when executed by the one or more processors cause the one or more processors to perform the steps of registering the plurality of nodes, determining whether the nodes are authorized to produce and authorized to receive certain events corresponding to objects of the directory, distributing the group session key to the nodes via a message, the message encapsulating the group session key according to a prescribed format, and selectively reregistering the nodes in response to updating the group session key.

20. (Amended) The computer system as recited in Claim 19, wherein the directory [server] is collocated with the event server, the directory [server] and the event server participating in a common one of the multicast groups.

21. (Unamended) The computer system as recited in Claim 19, wherein the prescribed format of the message conforms with light weight directory access protocol (LDAP).

22. (Unamended) The computer system as recited in Claim 19, wherein the directory authenticates by using authentication services of the directory in conjunction with a Kerberos service that allows extending membership to the multicast groups to nodes with no objects in the directory.

23. (Amended) The computer system as recited in Claim 19, wherein the event server manages the private keys of the plurality of nodes.

24. (Amended) The computer system as recited in Claim 19, wherein the event server updates the group session key by performing the steps of:

creating a new group session key;

modifying the [objects] object based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

25. (Unamended) The computer system as recited in Claim 19, wherein the computer system performs access control check of the nodes during registration.

26. (Amended) A computer-readable medium carrying one or more sequences of instructions for securely establishing communication in a multicast group of nodes of a network, in which the network includes publisher nodes, subscriber nodes, a multi-master directory that stores information about events in the network and that can authenticate the subscriber nodes and the publisher nodes, whereby each of the subscriber nodes and the publisher nodes receives a unique private key and that can determine events that the subscribers and the publishers may process, wherein execution of the one or more sequences of instructions by one or more processors causes the one or more processors to perform the steps of:

registering the subscribers and the publishers with an event server, the event server determining whether the publishers are authorized to produce certain events corresponding to [the] event types and whether the subscribers are authorized to receive the certain events in response to the step of [accessing] registering; and

generating a group session key for establishing [one of] the multicast [groups] group, the group session key being encrypted in a first message that has a prescribed format.

27. (Amended) A computer-readable medium as recited in Claim 26, further comprising the steps of:

receiving a second message from the subscribers in response to the subscribers determining whether the first message corresponds to a correct key version;

updating the group session key; and

selectively reregistering the subscribers at the event server.

28. (Amended) A computer-readable medium as recited in Claim 26, wherein the [step of authenticating comprises] directory authenticates by controlling access [by the directory] in conjunction with utilizing an external authentication service that allows extending membership of the multicast groups to subscribers with no corresponding objects in the directory.

29. (Amended) A computer-readable medium as recited in Claim [26] 27, wherein the step of updating comprises:

creating a new group session key;

modifying [the objects] an object in the directory based upon the new group session key by using a change password protocol;

sending a new message that contains the new group session key to the subscribers; and

notifying the subscribers to reregister.

30. (Unamended) A computer-readable medium as recited in Claim 26, wherein the step of registering comprises performing access control check of the subscribers by the event server.